Zu häufige Ausfallzeiten? Mit diesen Maßnahmen sorgen Sie für reibungslosen Netzwerkbetrieb

Die Vernetzung von Computern bringt höhere Flexibilität für alle Anwender. Wenn allerdings Probleme auftreten, steht meist der gesamte Betrieb still und schnelle Abhilfe ist gefragt. Das Wissen, an welchen Stellen Sie nachschauen müssen, um Probleme – schon im Vorfeld – zu erkennen, kann viel Zeit einsparen. Nicht immer sind es schwerwiegende Fehler, die ein Netzwerk zum Erliegen bringen: der Teufel steckt oft im Detail.

von Frank Erhardt

Inhalt **Seite**

Mit den Informationen aus diesem Beitrag können Sie

- schnell die Netzwerkunterbrechung auf den Verbindungsaufbau oder die Namensauflösung zurückführen und die Störung dauerhaft bereinigen,
- die häufigsten Konflikte im Netzwerk gezielt analysieren und so für einen reibungslosen Arbeitsablauf sorgen,
- den Netzwerkverkehr protokollieren und auswerten, um auch schwierige Probleme in den Griff zu bekommen.

Den Problemen auf den Grund gehen: Tools für die Fehleranalyse

Der erste Schritt zur Diagnose

Mit der folgenden Tabelle gewinnen Sie einen Überblick über die zusätzlichen Tools in der Microsoft-TCP/IP-Implementierung. Einige Netzwerkprobleme lassen sich mit ihrer Hilfe und den Anwendungsempfehlungen schneller beseitigen:

Tools	Anwendung
ARP	Prüft den ARP-Cache des internen Netzwerkadapters auf ungültige Einträge.
IPCONFIG	Zeigt die aktuelle TCP/IP-Konfiguration des Rechners an. Nutzen Sie das Tool, um DHCP-Leases freizugeben/zu erneuern.
NBTSTAT	Überprüft den aktuellen Status von NetBIOS über TCP/IP und aktualisiert den NetBIOS-Name-Cache. Damit lassen sich auch die registrierten Namen und Scope-IDs bestimmen.
NETSTAT	Zeigt Statistiken für die aktuellen TCP/IP-Verbindungen an.
NETDIAG	Prüft die Einstellungen der Netzwerkverbindungen.
NSLOOKUP	Überprüft Einträge, Alias-Namen, Domain-Host-Services und Betriebssystem-Infos durch Abfrage des DNS-Servers.
PING	Verschickt ICMP-Requests zur Prüfung, ob TCP/IP korrekt konfiguriert und das gewählte System verfügbar ist.
ROUTE	Zum Anzeigen, Ändern und Setzen der IP-Routing-Tabelle des Systems.
TRACERT	Verfolgt den Netzwerkpfad zu einem anderen System.
HOSTNAME	Zeigt den aktuellen Namen des Rechners an, auf welchem ein Befehl ausgeführt wird.

Wie Sie die Tools im Detail einsetzen, lesen Sie im Beitrag „T 100 – TCP/IP-Konfiguration“.

Einsatz des Netzwerkmonitors

Für den Fall, dass Sie durch die Nutzung der aufgelisteten Programme zu keiner Lösung kommen, stellt Microsoft den

Netzwerkmonitor zur Verfügung. Mit ihm lässt sich der gesamte Netzwerkverkehr zwischen zwei oder mehreren Systemen protokollieren und auswerten. Lesen Sie, wie Sie den Netzwerkmonitor installieren, benutzen und die erhaltenen Daten auswerten.

TCP/IP streikt! Mit dem Fragenkatalog zur schnellen Diagnose

Wichtige Fragestellungen vor der Problemlösung

Nutzen Sie nachfolgenden Fragenkatalog, um der Fehlerursache schneller auf den Grund zu kommen. Gelingt es, das Problem näher einzugrenzen, liegt auch die Lösung meist nicht mehr fern!

1. Welche Anwendung funktioniert nicht bzw. noch? Welcher Befehl wird nicht mehr ausgeführt?
2. Liegt es an der Namensauflösung oder IP-Verbindung, wenn das Problem auftaucht? Wenn es an der Namensauflösung liegt: Benutzt die Anwendung NetBIOS-Namen, DNS-Namen oder Hostnamen?
3. Wie sind die funktionierenden und nicht funktionierenden Anwendungen miteinander verbunden?
4. Haben die Anwendungen, die jetzt nicht mehr funktionieren, vorher auf diesem Computer oder im Netzwerk funktioniert?
5. Wenn die Anwendungen vorher funktioniert haben, welche Einstellungen wurden seitdem geändert?



Problem einkreisen

Identifizieren Sie zuerst die Anwendung oder Funktion, welche Probleme bereitet, z.B. Telnet, Internet Explorer, net use, net send, FTP. Haben Sie ermittelt, welche Anwendung Probleme verursacht, kreisen Sie die Fehlerquelle weiter ein:

Prüfen Sie, ob es sich um ein Problem mit der Auflösung des NetBIOS-Namens oder um ein Problem mit der Auflösung des Hostnamens handelt.

Applikationen und ihre Anwendungen:

NetBIOS-Anwendungen	Sockets/WinSockets-Anwendungen
1. Die verschiedenen **NET**-Kommandos 2. Windows NT-Administrator-Tools	1. Telnet 2. FTP 3. Web Browser

Schwierigkeiten beim Verbindungsaufbau oder falscher Namensauflösung: Hier bleibt kein Fehler unentdeckt

„System Error 53" – Fehlermeldungen

Häufig tritt bei Problemen mit der NetBIOS-Namensauflösung eine „System Error 53 occured"-Fehlermeldung auf, wenn Sie den Befehl **NET USE** verwenden. In diesem Fall ist die Namensauflösung für einen bestimmten Computer-Namen fehlgeschlagen. Die Fehlermeldung kann aber auch erscheinen, wenn ein Problem beim Aufbau der NetBIOS-Verbindung aufgetreten ist. So ermitteln Sie den Ursprung der Fehlermeldung:



1. Öffnen Sie die Eingabeaufforderung und geben Sie folgenden Befehl ein: **NET VIEW \\\\<IP-Adresse>**.

Verbindung prüfen

Wenn dieses Kommando fehlschlägt, hängt das mit dem Aufbau einer Verbindung zusammen. Ziehen Sie den Fehlersuchbaum auf Seite N 250/06 zu Rate, der die Lösung solcher Verbindungsprobleme beschreibt.

Hostnamen prüfen

2. Öffnen Sie die Eingabeaufforderung und geben Sie Folgendes ein: **NET VIEW \\\\<HOSTname>**.

Funktioniert dies nicht, scheint die Namensauflösung fehlerhaft zu sein. Lesen Sie dazu die nachfolgenden Abschnitte, die sich mit der Lösung von fehlerhafter Namensauflösung beschäftigen.

Überprüfen Sie die Einträge der LMHOSTS-Datei

Fehlerhafte Namensauflösung in der LMHOSTS-Datei

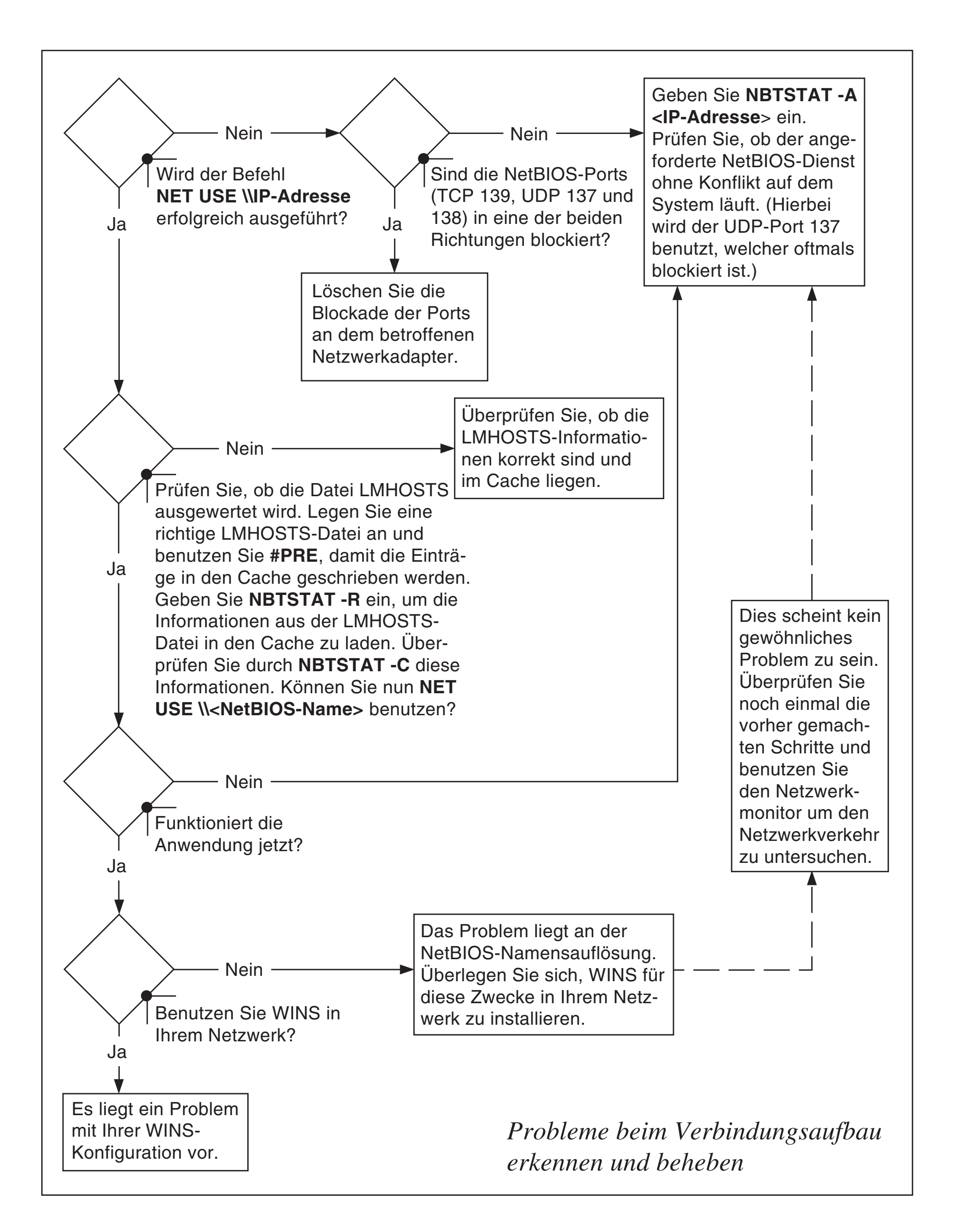
Wenn Sie Probleme mit der Auflösung von Netzwerknamen haben, kann dies an den Einträgen oder der Lage der LMHOSTS-Datei liegen. Diese Datei löst IP-Adressen in NetBIOS-Namen auf. Sie finden die LMHOSTS-Datei in folgendem Verzeichnis: \%Systemroot%\System32\Drivers\Etc. Wie auch bei der HOSTS-Datei werden die Einträge von oben nach unten durchsucht. Wenn dabei ein Eintrag doppelt vergeben wurde, wird der erste in der Liste benutzt, egal ob dieser korrekt ist oder nicht. Welche LMHOSTS-Datei für die Namensauflösung vom System verwendet wird, bestimmt ein Eintrag in der Registry. So prüfen Sie den Eintrag und passen die richtige LMHOSTS-Datei für Ihr System an:

1. Öffnen Sie den Registry Editor durch „**Ausführen**" und Eingabe von **REGEDT32.EXE**.
2. Wechseln Sie zu folgendem Schlüssel in der Registry: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\databasepath.
3. Der dort angegebene Pfad gibt dem lokalen Rechner an, wo er die LMHOSTS-Datei finden kann.

Detektivisch nach dem Ausschluss-Prinzip: Schritt für Schritt zur Ursache

NET USE \\IP-Adresse nicht ausgeführt

Gehen Sie nun anhand des Fehlersuchbaums vor um den Fehler bei Verbindungsproblemen zu beheben:



Probleme beim Verbindungsaufbau erkennen und beheben

Fehlerhaften Verbindungsaufbau von Sockets-/ WinSockets-Anwendungen beheben

Die Namensauflösung überprüfen

Wenn eine Anwendung, die Windows-Sockets nutzt, nicht einwandfrei funktioniert, liegt die Ursache in

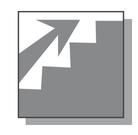
- der DNS-Konfiguration,
- der WINS-Konfiguration oder
- der HOSTS-Datei.

Eine nicht einwandfrei durchgeführte Namensauflösung erkennen Sie daran, dass Verbindungen über die IP-Adresse funktionieren, nicht aber Verbindungen über den Hostnamen des anderen Systems.

Überprüfen der WINS-Konfiguration

Systemeinstellung korrekt?

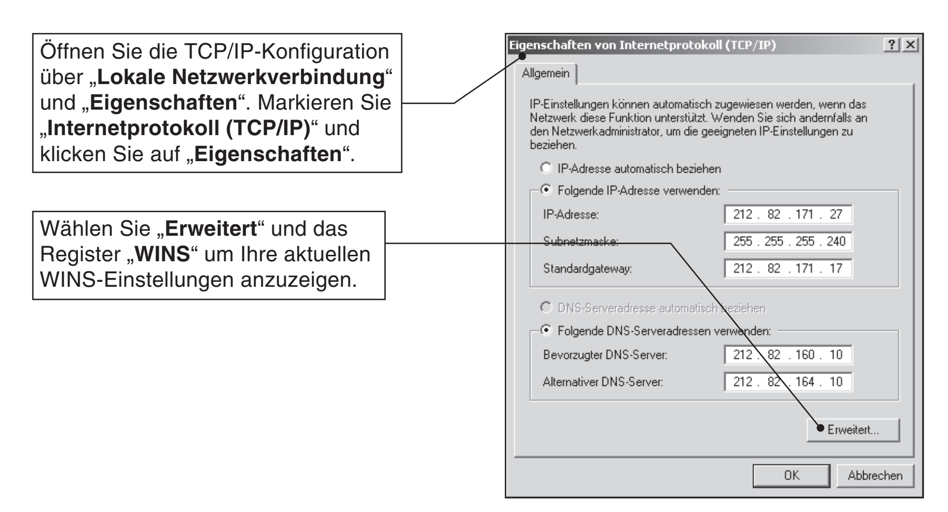
Wenn Sie WINS-Server in Ihrem Netzwerk verwenden, müssen die Clients entsprechend eingerichtet werden, damit die Namensabfrage und die automatische Registrierung der Computernamen auf dem Server einwandfrei funktionieren. Die nächsten Schritte beschreiben auf einfache Weise die Kontrolle Ihres Systems:



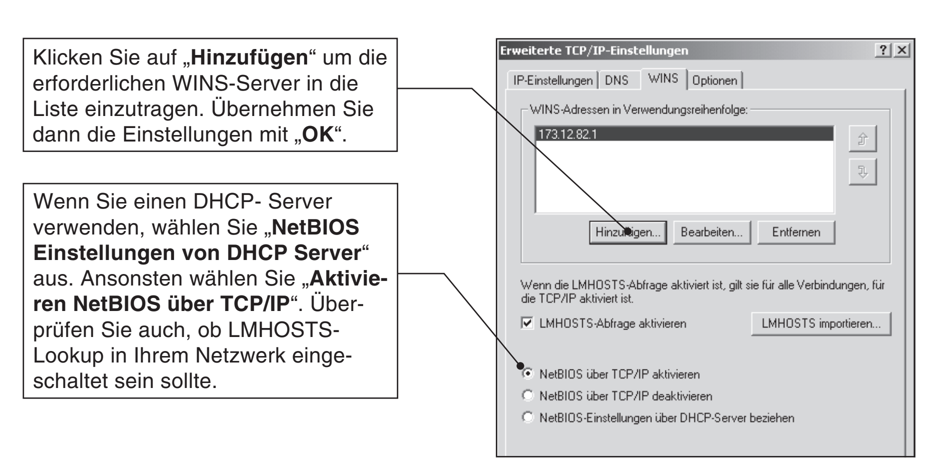
1. Öffnen Sie in der Systemsteuerung die „**Netzwerkeigenschaften**“.
2. Überprüfen Sie nun die Angaben zu den WINS-Servern. Falls kein Server in der Liste auftaucht, fügen Sie diesen hinzu.

Vorsicht bei DHCP-Clients

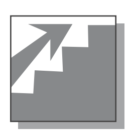
Verwenden Sie auf Ihrem Rechner DHCP zur automatischen Zuweisung einer IP-Adresse, sollten in der Liste keine WINS-Server aufgeführt sein. Diese Clients bekommen normalerweise die Adressen der WINS-Server automatisch zugewiesen.



Die Eigenschaften von TCP/IP



Hinzufügen der WINS-Server



3. Überprüfen Sie auf einem DHCP-Client, ob die WINS-Server korrekt aufgeführt sind. Geben Sie in der Eingabeaufforderung den Befehl **IPCONFIG /ALL** ein.

Wenn die Einträge nicht stimmen, müssen auf dem DHCP-Server die Angaben korrigiert werden. Starten Sie den Rechner neu, damit die neuen Einstellungen wirksam werden.

Client-Einträge für den DNS-Dienst kontrollieren

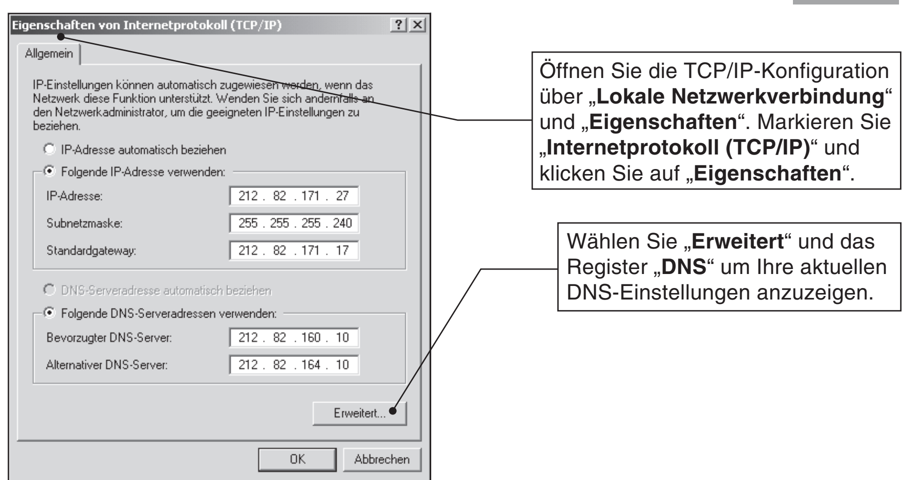
Netzwerkeigenschaften prüfen

Damit die Domain-Namen in IP-Adressen umgesetzt werden können, muss auf dem Client mindestens ein DNS-Server eingetragen sein.

Fehlende oder falsche DNS-Server-Einstellungen machen Sie so ausfindig:

1. Öffnen Sie in der Systemsteuerung die „**Netzwerkeigenschaften**".



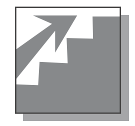


Eigenschaften von TCP/IP

2. Überprüfen Sie nun die Angaben zu den DNS-Servern. Falls kein Server in der Liste auftaucht, fügen Sie diesen hinzu.

DHCP-Client und DNS-Server-Einträge

Verwenden Sie auf Ihrem Rechner DHCP für eine automatische Zuweisung einer IP-Adresse, sollten in der Liste keine DNS-Server aufgeführt sein. Diese Clients bekommen normalerweise die Adressen der DNS-Server automatisch zugewiesen.



3. Überprüfen Sie auf einem DHCP-Client, ob die DNS-Server korrekt aufgeführt sind. Geben Sie hierzu in der Eingabeaufforderung den Befehl **IPCONFIG /ALL** ein.

Falsche Eintragungen korrigieren Sie direkt auf dem DHCP-Server. Starten Sie danach den Rechner neu, damit die neuen Einstellungen wirksam werden.

HOSTS-Datei auf dem Client überprüfen

Einträge analysieren

Wenn Sie auf ein anderes System nicht über dessen Namen zugreifen können und eine HOSTS-Datei für die Namensauflösung benutzen, liegen die Probleme wahrscheinlich an den Einträgen in dieser Datei. Die HOSTS-Datei wird genutzt, um Computernamen IP-Adressen zuzuordnen. Sie finden die Datei im Verzeichnis: \%Systemroot%\System32\Drivers\Etc.

Diese Datei ist statisch, Sie müssen also alle Einträge manuell vornehmen. Ihr Inhalt sollte wie folgt aussehen:

IP Adress	Friendly Name
192.10.10.50	testpc01
192.10.10.51	testpc02
127.0.0.1	localHOST

Folgende Probleme in der HOSTS-Datei können Netzwerkfehler hervorrufen und sollten von Ihnen überprüft werden:

- In der HOSTS-Datei ist der Computername nicht eingetragen.
- Der Rechnername in der HOSTS-Datei ist falsch geschrieben.
- Die IP-Adresse für den Rechnernamen ist ungültig oder falsch.
- Die HOSTS-Datei beinhaltet mehrere Einträge für den gleichen Rechner. Da diese Datei von oben nach unten gelesen wird, wird der erste gefundene Eintrag genutzt.

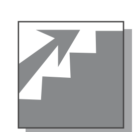
Der Fehlersuchbaum auf Seite N 250/12 zeigt, welche Schwierigkeiten im Zusammenhang mit der Namensauflösung auftreten können und wie diese behoben werden.

IP-Verbindungskonflikte schnell einkreisen und sicher beheben

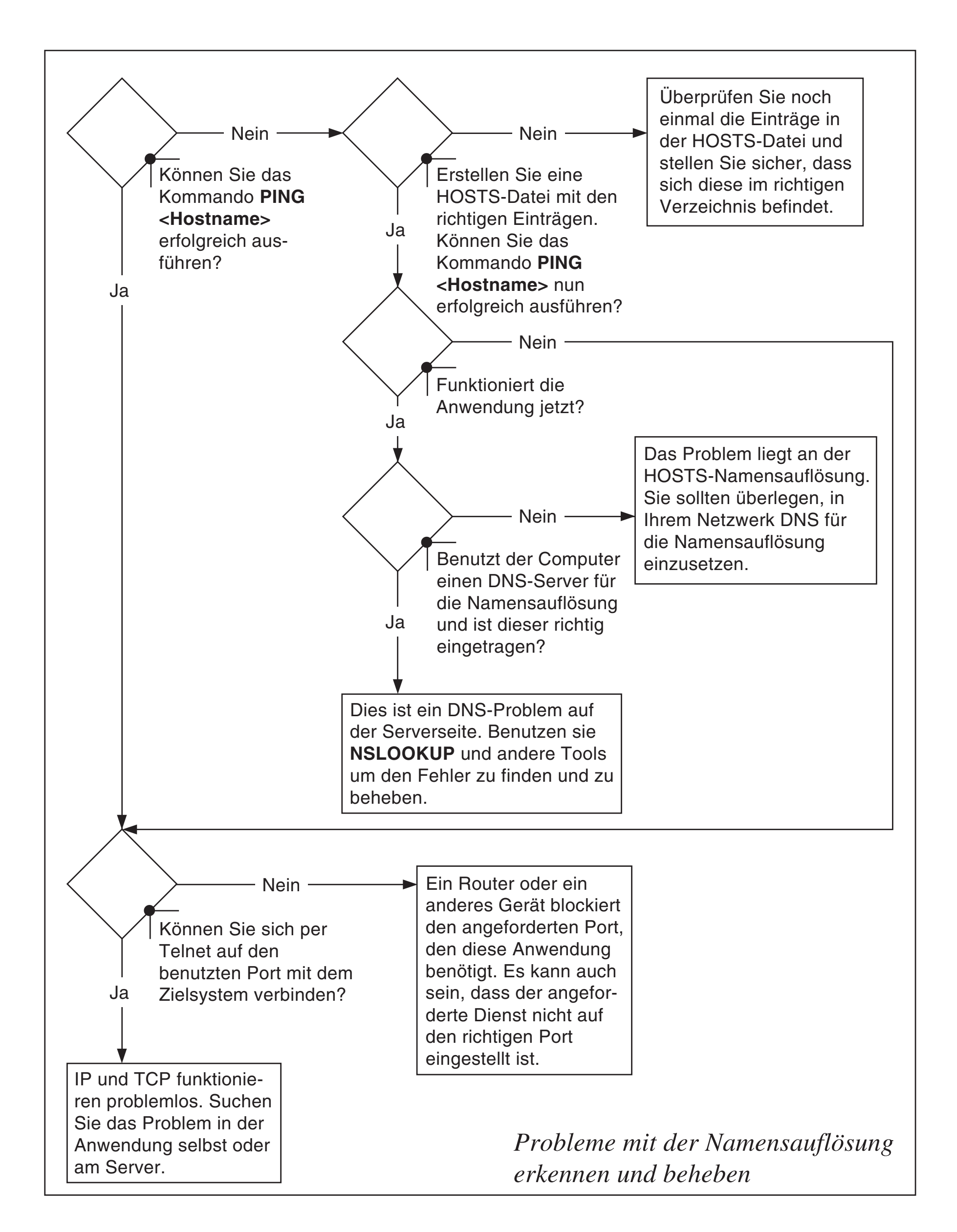
Fehlerhafte IP-Konfiguration

Wenn das Problem nicht an der Namensauflösung liegt, kann auch eine falsche IP-Konfiguration auf Ihrem Rechner die Ursache sein. Grundsätzlich sollten Sie wie folgt vorgehen, um TCP/IP-Probleme zu finden und zu beheben:

1. Überprüfen Sie, ob die IP-Konfiguration des Rechners richtig ist.



Nutzen Sie das Kommando **IPCONFIG** auf dem Rechner. Um die gesamte Konfiguration zu sehen, geben Sie **IPCONFIG / ALL** ein. Die Ausgabe dieses Kommandos können Sie durch Eingabe von **IPCONFIG /ALL > <Verzeich-nis\Dateiname>** in eine Datei kopieren um diese später auszuwerten. Der Inhalt der Datei erscheint dann wie auf Seite N 250/13 dargestellt.



Probleme mit der Namensauflösung erkennen und beheben

Analyse der IP-Konfiguration mit IPCONFIG

Windows 2000 IP Configuration

HOST Name . . . . :	cbspc001
Primary DNS Suffix . . . . :	CBS2000.HAMBURG.DE
Node Type . . . . :	Hybrid
IP Routing Enabled . . . . :	No
WINS Proxy Enabled . . . . . . :	No
DNS Suffix Search List . . . . . :	CBS2000.HAMBURG.DE HAMBURG.DE

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :	
Description . . . . :	NETGEAR FA311 Fast Ethernet PCI Adapter
Physical Address . . . . :	00-02-E3-05-A2-F9
DHCP Enabled . . . . :	Yes
Autoconfiguration Enabled . . . . :	Yes
IP Address. . . . . :	10.1.0.23
Subnet Mask . . . . :	255.0.0.0
Default Gateway . . . . :	10.1.0.2
DHCP Server . . . . :	10.1.0.1
DNS Servers . . . . :	10.1.0.1 10.1.0.2
Primary WINS Server . . . . :	10.1.0.1
Secondary WINS Server . . . . . . :	10.1.0.2
Lease Obtained. . . . . :	Donnerstag, 28. Juni 2002 21:51:20
Lease Expires . . . . :	Freitag, 6. Juli 2002 21:51:20

Doppelte IP-Adressen: IPCONFIG zeigt den Adresskonflikt an

Analyse von Adresskonflikten

Wenn Sie Ihrem Rechner eine IP-Adresse gegeben haben, die schon von einem anderen Client im Netzwerk benutzt wird, wird die Subnet-Mask als „0.0.0.0“ angegeben.

Lösung

Verwenden Sie eine freie IP-Adresse oder einen DHCP-Server um dieses Problem zu lösen.

Das Diagnose-Tool DHCP findet fehlerhafte Zuweisungen von IP-Adressen

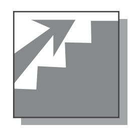
Standard-IP-Adressen beim Scheitern der DHCP-Anfrage

Wenn die IP-Adresse Ihres Rechners die Form „169.254.x.y“ hat, wurde Ihnen eine IP-Adresse von Windows 2000 zugewiesen. Dies liegt daran, dass die Anfrage an den DHCP-Server, Ihrem Rechner eine IP-Adresse zuzuweisen, gescheitert ist.

Überprüfen Sie jetzt die Server-Konfiguration und testen Sie, ob genügend Adressen für die automatische Verteilung zur Verfügung stehen. Ist dies der Fall, fahren Sie mit dem Fehlersuchbaum auf Seite N 250/15 fort, um die physikalische Erreichbarkeit der DHCP-Server zu testen.

Testen der physikalischen Verbindung

Wenn Sie keine Fehler in der IP-Konfiguration entdecken können, fahren Sie wie folgt fort:



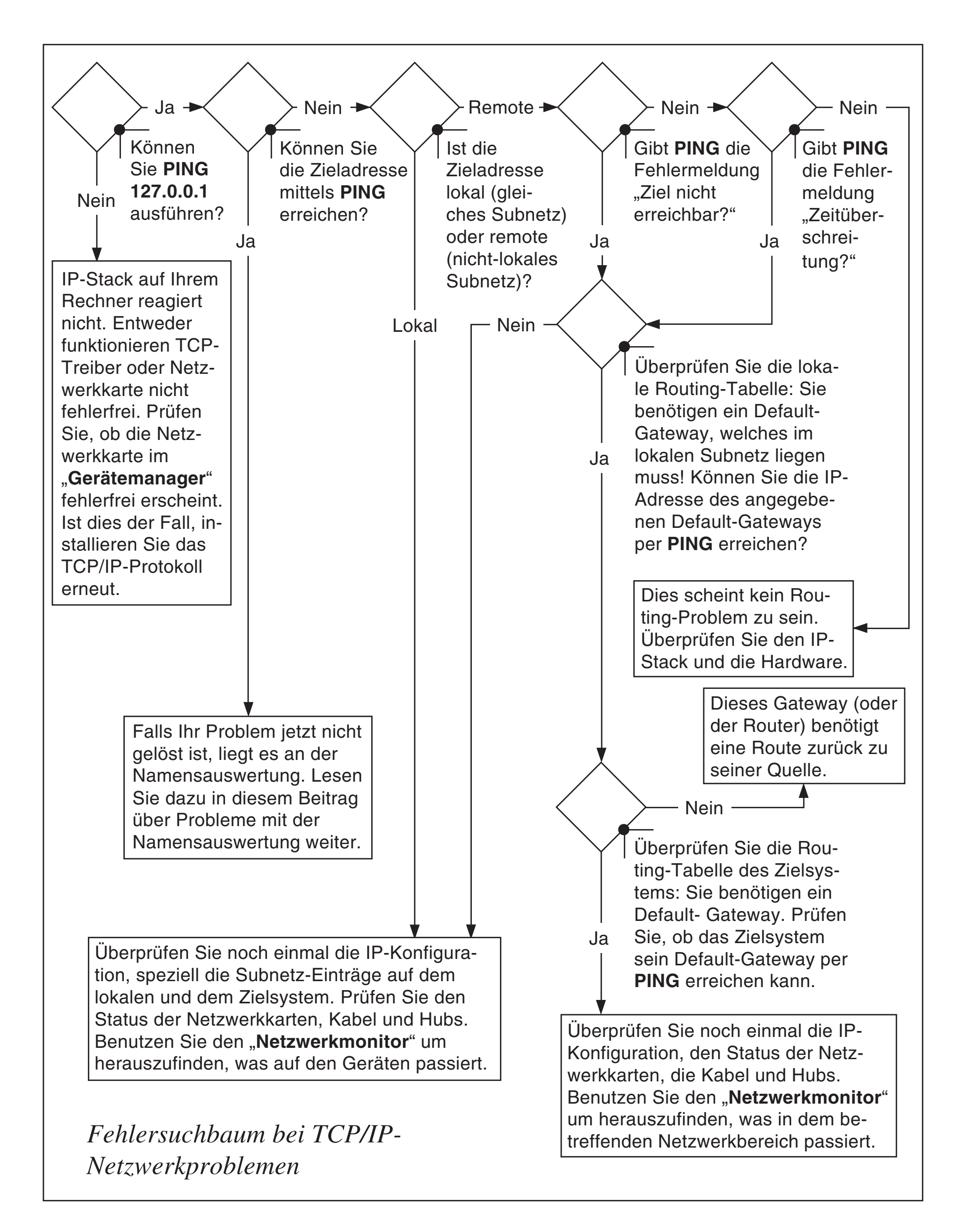
Testen Sie, ob Sie mit anderen Rechnern im TCP/IP-Netzwerk eine Verbindung aufbauen können.

Nutzen Sie den Fehlersuchbaum zu TCP/IP-Netzwerkproblemen auf Seite N 250/15 zur Fehlererkennung und -lösung.

Testen Sie die IP-zu-MAC-Adressenauflösung mittels ARP

ARP für die eindeutige Hardware-Adresse

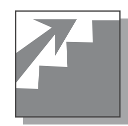
In einem Netzwerk werden Ressourcen über IP-Adressen, Hostnamen oder NetBIOS-Namen angesprochen. Egal welche Namenskonvention in Ihrem Netzwerk gilt, die Zieladresse muss in eine Hardware-Adresse (MAC-Adresse) aufgelöst werden. Diese Funktionalität wird durch das ARP (Adress Resolution Protocol) sichergestellt.



Fehlersuchbaum bei TCP/IP-Netzwerkproblemen

Doppelte Adressen erkennen

Es kann vorkommen, dass in einem Netzwerk zwei Rechner dieselbe IP-Adresse benutzen. Überprüfen Sie dies mit dem ARP-Tool:



1. Geben Sie **ARP -A** in der Eingabeaufforderung ein um die ARP-Tabelle anzuzeigen.
2. Dort erkennen Sie, ob IP-Adressen doppelt vergeben sind.
3. Löschen Sie diese gegebenenfalls durch **ARP -D <IP Adresse>**.

Das Ereignisprotokoll als Spürnase

Haben Sie keine Einträge gefunden, die für die Fehler verantwortlich sein könnten, kann ein Blick in das Ereignisprotokoll Klarheit bringen.



Öffnen Sie die „**Ereignisanzeige**“ und prüfen Sie die Liste auf DHCP-Meldungen.

Wenn DHCP einen doppelten Namen im Netzwerk findet, wird der Zugriff auf die Netzwerkkarte verhindert. Solche und andere DHCP-Meldungen finden Sie im Ereignisprotokoll. Meistens geben diese Aufschluss darüber, wo die Probleme liegen.

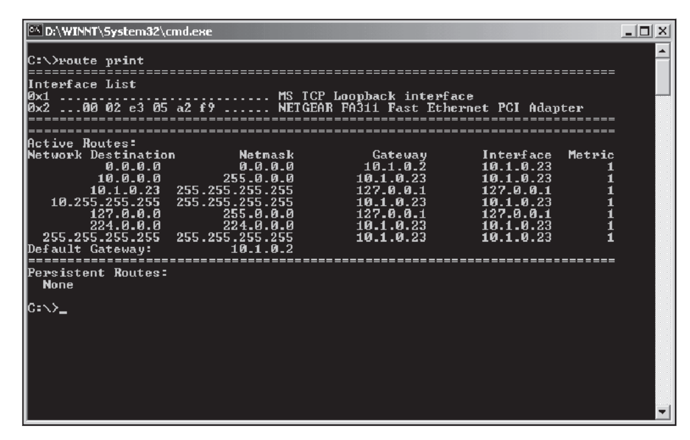
Probleme lösen mit dem IP-Routing

Routing-Tabelle befragen

Damit Ihr Rechner Zugriff auf Systeme außerhalb Ihres lokalen Subnetzes haben kann, muss eine Route oder ein Default-Gateway in der Routing-Tabelle angegeben sein, die Ihrem Rechner den Weg zum Zielsystem zeigen.



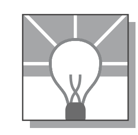
Öffnen Sie die Eingabeaufforderung und geben Sie **ROUTE PRINT** ein um die Routing-Tabelle Ihres PCs anzuzeigen.



Anzeigen der lokalen Routing-Tabelle

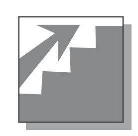
Gateway-Test mit PING

Der erste Eintrag in der Tabelle gibt dem Rechner an, welches Gateway er für alle nicht-lokalen Netzwerke nutzen soll. Prüfen Sie, ob dieser Eintrag richtig ist und Sie dieses Gateway mittels **PING** erreichen können.



Sie können die Routen auch mit dem **TRACERT**-Kommando verfolgen. Damit erhalten Sie nicht nur Informationen über existente Gateways, sondern auch über den Weg zum Ziel. Außerdem werden Hinweise auf Fehlerrouten bzw. nicht routende Gateways angezeigt. Falls der Eintrag nicht korrekt ist, kontrollieren Sie die TCP/IP-Konfiguration Ihres Rechners noch einmal oder überprüfen Sie die Einstellungen auf dem DHCP-Server.

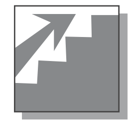
Möchten Sie eine feste Route zur Routing-Tabelle Ihres Rechner hinzufügen, gehen Sie wie folgt vor:



Geben Sie folgendes Kommando ein: **ROUTE ADD <Zielnetzwerk-Adresse> MASK <Subnet-Mask des Zielnetzwerkes> < IP-Adresse des Routers, der zum Erreichen des Zielnetzes benutzt werden soll>**.

Routing auf dem Gateway

Haben Sie auf Ihrem lokalen Rechner alle Einstellungen überprüft und kein Problem mehr gefunden, ist auf dem Gateway eventuell IP-Routing nicht aktiviert. Handelt es sich bei Ihrem Gateway um einen Windows 2000-Rechner, wird IP-Routing standardmäßig ausgeschaltet. Aktivieren Sie den IP-Router wie folgt:



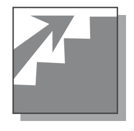
1. Öffnen Sie den Registrierungseditor.
2. Gehen Sie zu folgendem Schlüssel: HKEY_LOKAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters.
3. Dort suchen Sie auf der rechten Fensterseite den Schlüssel IPEnableRouter.
4. Öffnen Sie den Schlüssel und geben Sie im Eingabefeld den Wert **1** ein.

Starten Sie den Rechner sicherheitshalber neu, damit die Einstellung wirksam wird.

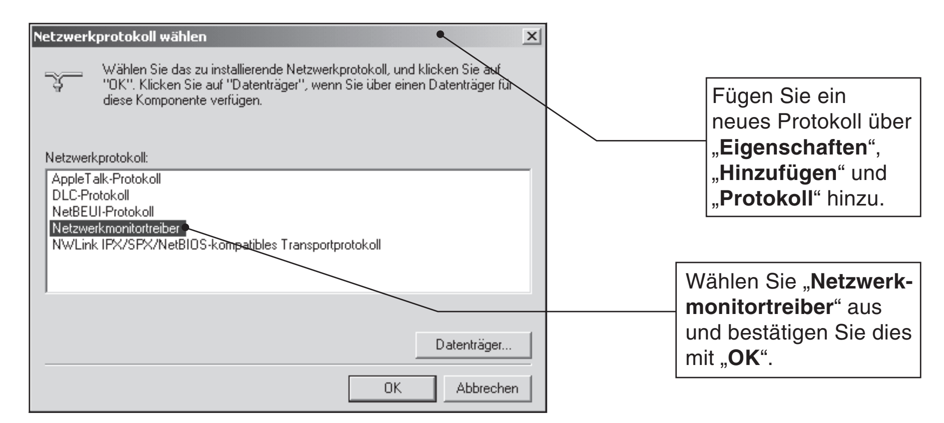
Der Microsoft-Netzwerkmonitor: Das Programm für eine professionelle Analyse des Netzwerktraffics

Netzwerkmonitor und Client-Treiber installieren

Damit Sie mit dem Netzwerkmonitor den Netzwerkverkehr überprüfen können, muss dieser auf einem Server installiert sein. Zusätzlich ist auf jedem Client, dessen Netzwerkverkehr mitanalysiert werden soll, der Netzwerkmonitor-Treiber zu installieren. So installieren Sie die benötigten Komponenten für den Netzwerkmonitor auf allen relevanten Rechnern:



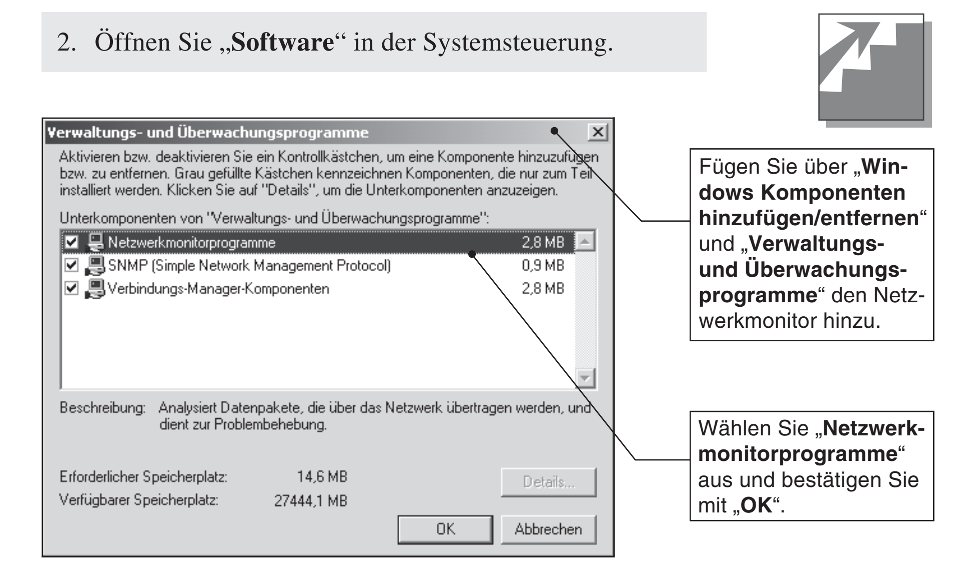
1. Gehen Sie auf die Eigenschaften Ihrer lokalen Netzwerkverbindung über die „**Systemsteuerung**“.



Installation des Netzwerkmonitor-Treibers

Damit kann ab jetzt der Netzwerkverkehr Ihres Rechners über den Netzwerkmonitor mitgelesen und ausgewertet werden. Den Netzwerkmonitor selbst installieren Sie wie folgt:

2. Öffnen Sie „**Software**“ in der Systemsteuerung.



Installation des Netzwerkmonitors

Beachten Sie, dass der Netzwerkmonitor nur auf Windows Server-Systemen zur Verfügung steht und nur dort installiert werden kann.

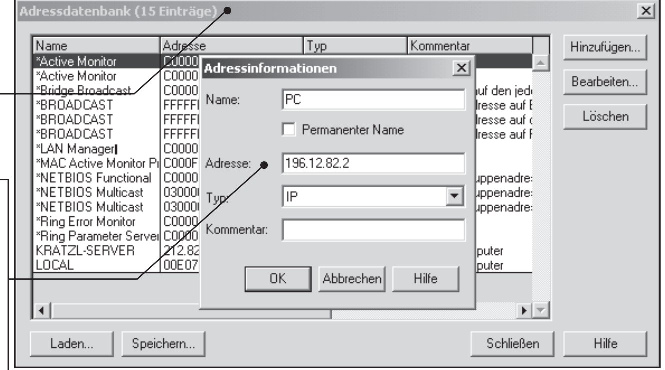
Richtige Konfiguration des Netzwerkmonitors

Damit Sie den Netzwerkverkehr zwischen zwei oder mehr Systemen aufzeichnen können, müssen Sie zuerst einige Einstellungen im Netzwerkmonitor vornehmen:

1. Starten Sie den Netzwerkmonitor im Programm-Menü.

Fügen Sie die Adressen der Zielsysteme über „**Hinzufügen**“ und „**Adressen**“ hinzu.

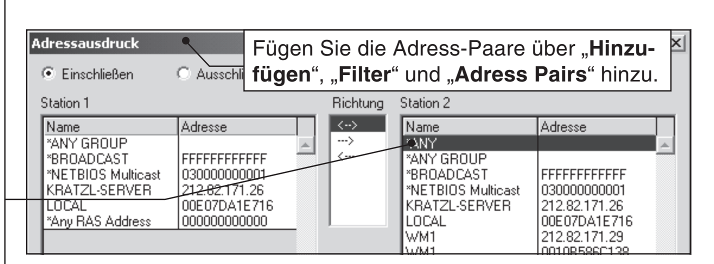
Geben Sie hier die IP-Adresse des Zielsystems ein und bestätigen Sie dies mit „**OK**“. Führen Sie diesen Schritt für alle Systeme durch, die Sie analysieren möchten.



Eingabe der Zieladressen im Netzwerkmonitor

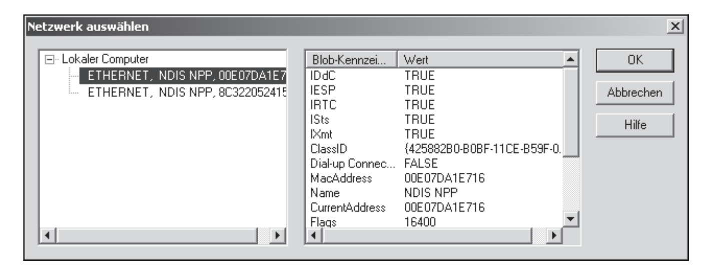
2. Geben Sie im nächsten Schritt die Adresspaare ein, die überwacht werden sollen.

Hier können Sie bestimmen, welche Art von Netzwerkverkehr mitprotokolliert werden soll. Wählen Sie am Anfang „**ANY**“ und „**ANY GROUP**“ aus, um den gesamten Netzwerkverkehr aufzuzeichnen.



Eingabe der Adress-Paare für die Analyse

3. Geben Sie ein, auf welchem Netzwerkadapter mitprotokolliert werden soll.



Auswahl des Netzwerkadapters für die Protokollierung

Start und Auswerten der Überwachung

Um den Netzwerkverkehr zwischen den vorher angegebenen Systemen zu überwachen, gehen Sie auf „**Hinzufügen**“ und „**Start**“. Zum Beenden und Auswerten des Protokolls wählen Sie „**Hinzufügen**“ und „**Stop and View**“.

Beispiel: WINS-Anforderung

Dem folgenden Netzwerkmonitor-Mitschnitt einer WINS-Anfrage können Sie entnehmen, welche Einträge entscheidend sind. Probleme in Ihrem Netzwerk erkennen Sie so anhand der Unterschiede gleich und können die Fehler sofort beheben.

Die entscheidenden Einträge auf einen Blick

Frame	Time	Src MAC Address	Dst MAC Address	Protocol	Description	Vorgang
1	10.947	CLIENT	PDC	NBT	NS: Refresh req. for TESTPC<00>	Der Client kontaktiert den PDC mit der Anfrage auf einen Refresh. Workstation namens TESTPC (<00> = Workstation-Namens-Registrierung).
2	10.954	CLIENT	PDC	ARP_ RARP	ARP: Reply, Target IP: 10.25.25.25 Target Hdwr Addr: 000082338674	Der Client sendet dem PDC die notwendigen Informationen für den Vorgang.

Frame	Time	Src MAC Address	Dst MAC Address	Protocol	Description	Vorgang
3	10.954	PDC	CLIENT	NBT	NS: Registration (Node Status) resp. for TESTPC<00>, Success, Owner Addr. 10.25.25.100	Der PDC meldet dem Client, dass die erneute Eintragung erfolgreich war.
4	10.955	CLIENT	PDC	NBT	NS: Refresh req. for CLIENT	Der Client kontaktiert den PDC mit der Anfrage auf eine Refresh-WINS-Eintragung für den Client-Rechner.
5	10.977	PDC	CLIENT	NBT	NS: Registration (Node Status) resp. for CLIENT, Success, Owner Addr. 10.25.25.100	Der PDC meldet dem Client, dass die erneute Eintragung erfolgreich war.
6	10.978	CLIENT	PDC	NBT	NS: Refresh req. for CLIENT <03>	Der Client stellt die Anfrage an den PDC, den Nachrichtendienst (<03> = Nachrichtendienst NetDDE-Registrierung) erneut zu registrieren.
7	11.003	PDC	CLIENT	NBT	NS: Registration (Node Status) resp. for CLIENT <03>, Success, Owner Addr. 10.25.25.100	Der PDC meldet dem Client, dass die erneute Eintragung erfolgreich war.
8	11.003	CLIENT	PDC	NBT	NS: Refresh req. for CLIENT <00>	Der Client kontaktiert den PDC mit der Anfrage auf einen Refresh. Workstation namens CLIENT(<00>= Workstation-Namens-Registrierung).
9	11.043	PDC	CLIENT	NBT	NS: Registration (Node Status) resp. for CLIENT <00>, Success, Owner Addr. 10.25.25.100	Der PDC meldet dem Client, dass die erneute Eintragung erfolgreich war.

Beachten Sie, dass die Zahl und der Typ der Registrierung von der Anzahl und Art der Dienste abhängen, die auf den Systemen laufen. Ein PDC produziert z.B. mehr WINS-Registrierungen als eine Workstation.